PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-173254

(43)Date of publication of application : 20.06.2003

(51)Int.Cl. G06F 7/58
G09C 1/00
H03K 3/84

(21)Application number : 2002-183967

(22)Date of filing : 25.06.2002

(71)Applicant : TOSHIBA CORP

(72)Inventor : FUJITA SHINOBU
UCHIDA KEN
KOGA JUNJI
OBA RYUJI

(30)Priority

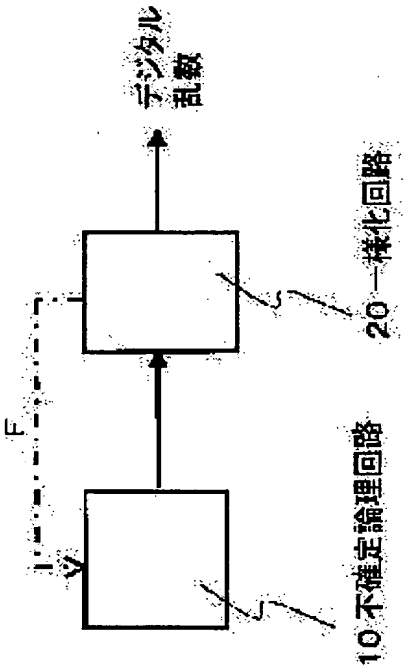
Priority number : 2001294836 Priority date : 26.09.2001 Priority country : JP

(54) RANDOM NUMBER FORMING CIRCUIT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a random number forming circuit generating random numbers having a high trueness degree, and transformable into a small integrated circuit.

SOLUTION: This random number forming circuit is provided with an indefinite logical circuit including a flip-flop type logical circuit for imparting a digital output value univocally undetermined to a digital input value, and a uniformizing circuit including an exclusive logical sum arithmetic circuit for equalizing an appearance frequency of '0' and '1' in the digital output value outputted from the indefinite logical circuit.



LEGAL STATUS

[Date of request for examination] 30.09.2003

[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3604674
[Date of registration]	08.10.2004
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

W9283

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－173254
（P2003－173254A）
(43)公開日　平成15年６月20日(2003.6.20)

(51)Int.Cl.'		識別記号	FI			テーマコード'(参考)
Ｇ０６Ｆ	7/58		Ｇ０６Ｆ	7/58	Ａ	５Ｊ０４９
Ｇ０９Ｃ	1/00	６５０	Ｇ０９Ｃ	1/00	６５０Ｂ	５Ｊ１０４
Ｈ０３Ｋ	3/84		Ｈ０３Ｋ	3/84	Ｚ	

審査請求　未請求　請求項の数８　ＯＬ　（全 15 頁）

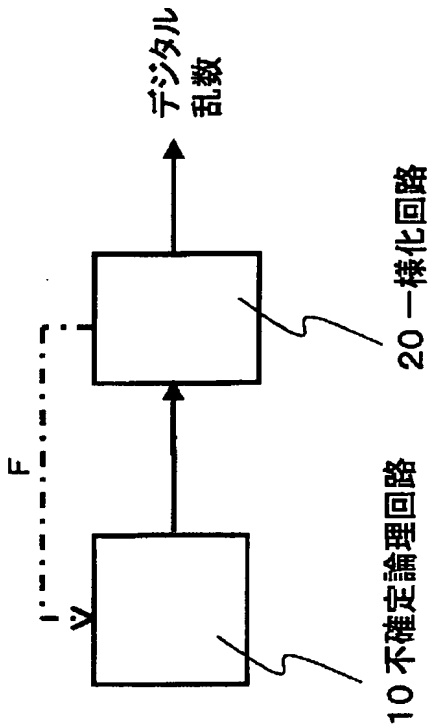
(21)出願番号　特願2002－183967(P2002－183967)
(22)出願日　平成14年６月25日(2002.6.25)
(31)優先権主張番号　特願2001－294836(P2001－294836)
(32)優先日　平成13年９月26日(2001.9.26)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　藤田　忍
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　内田　建
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝横浜事業所内
(74)代理人　100088487
弁理士　松山　允之　（外１名）

最終頁に続く

(54)【発明の名称】　乱数生成回路

(57)【要約】
【課題】　真性度の高い乱数を発生させ、かつ小型の集積回路化が可能な乱数生成回路を提供することを目的とする。
【解決手段】　デジタル入力値に対して一義的に決定されないデジタル出力値を与えるフリップフロップ型の論理回路を含む不確定論理回路と、前記不確定論理回路から出力される前記デジタル出力値における「０」と「１」の出現頻度を均等にするための排他的論理和演算回路などを含む一様化回路と、を備えた乱数生成回路を提供する。



【特許請求の範囲】
【請求項１】デジタル入力値に対して一義的に決定されないデジタル出力値を与えるフリップフロップ型の論理回路を含む不確定論理回路と、
前記不確定論理回路から出力される前記デジタル出力値における「０」と「１」の出現頻度を均等にするための一様化回路と、
を備えたことを特徴とする乱数生成回路。
【請求項２】前記不確定論理回路は、前記フリップフロップ型の論理回路の出力を前の状態を保持した出力とするための入力信号を継続的に与えつつ、前記フリップフロップ型の論理回路の前の状態に関する情報が実質的に消去される時間あるいはそれ以上の時間に亘って前記フリップフロップ型の論理回路に対する電源をオフするフェイズと、前記フリップフロップ型の論理回路に対する電源をオンするフェィズとを交互に繰り返すことにより、前記フリップフロップ型の論理回路から不確定なデジタル信号列を出力させることを特徴とする請求項１記載の乱数生成回路。
【請求項３】前記フリップフロップ型の論理回路は、ＲＳ型のフリップフロップであり、
前記不確定論理回路は、前記ＲＳ型のフリップフロップに対する入力Ｓ及び入力Ｒとして、前の状態を保持した出力を得るための入力データの組み合わせと、フリップフロップとして無効となる入力データの組み合わせと、を交互に入力することにより前記ＲＳ型のフリップフロップからの出力を連続的に不確定とすることを特徴とする請求項２記載の乱数生成回路。
【請求項４】前記一様化回路は、
前記フリップフロップ型の論理回路から出力される「０」と「１」の出現頻度をカウントするカウント回路と、
前記カウント回路によりカウントした前記出現頻度に基づいたフィードバック信号を前記フリップフロップ型の論理回路に与えるフィードバック回路と、
を有することを特徴とする請求項１～３のいずれか１つに記載の乱数生成回路。
【請求項５】前記一様化回路は、前記不確定論理回路から出力された複数のデジタル信号の排他的論理和を演算し、乱数として出力することを特徴とする請求項１～４のいずれか１つに記載の乱数生成回路。
【請求項６】前記一様化回路は、「０」と「１」との出現頻度が１：１であるデジタル信号列と、前記不確定論理回路から出力されるデジタル信号列と、の排他的論理和を演算し、デジタル乱数列として出力することを特徴とする請求項１～４のいずれか１つに記載の乱数生成回路。
【請求項７】前記不確定論理回路は、４つ以上の偶数のＮＯＲ回路またはＮＡＮＤ回路を含み、これらＮＯＲ回路またはＮＡＮＤ回路は、それぞれの回路の出力端子がその次の回路の入力端子の一方に連鎖的に接続されてなるものであることを特徴とする請求項１記載の乱数生成回路。
【請求項８】前記不確定論理回路は、複数のＲＳ型のフリップフロップを含み、これらフリップフロップ毎に大きさが異なるパルス電圧を入力し、これらフリップフロップからの出力の排他的論理的和を出力とするものであることを特徴とする請求項１記載の乱数生成回路。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、乱数生成回路に関し、特に、デジタル論理回路によりコンパクトに構成することが可能でしかも真性度が高い乱数を発生し、暗号アルゴリズムに用いても好適な乱数生成回路に関する。
【０００２】
【従来の技術】デジタル乱数は、確率過程を伴う現象のシミュレーションや、セキュリティーに用いる暗号アルゴリズムでの暗号鍵の生成などに用いられる。従来、デジタル乱数としては、ＣＰＵで計算によって作られる「擬似乱数」が用いられてきた。この疑似乱数は、典型的には、「フィードバックシフトレジスタ」と呼ばれる論理回路で作られる。
【０００３】これに対して、抵抗やダイオードに発生する雑音を使って乱数を作り出す方式も実用化されている。この場合、乱数に偏りや周期性などは見られなくなり、「真性乱数」に近いものが得られる。このタイプの乱数生成回路においては、雑音源の素子に一定電流を流して発生する雑音をハイパスフィルター回路に通して、ＡＣ成分を取り出し、それをアナログ回路で増幅したのち、ＡＤ変換してデジタル化する。このとき、ある値を閾値として、それを越えるものを「１」、それ以下のものを「０」というようにする。さらに、出てきた乱数列は偏りが出るため、それをデジタル回路で補正してから用いる場合が多い。
【０００４】
【発明が解決しようとする課題】ＣＰＵで作る擬似乱数は、初めに与えた数字（種）が同じであれば、同じ乱数を発生させてしまうことや、レジスタの個数に基づく周期性をもってしまうため、乱数としては適当でないことが知られている。特に、セキュリティーに用いる場合には、「暗号鍵」を破られる危険性を産む原因となる。
【０００５】一方、雑音を増幅するタイプだと、一般的に抵抗やダイオードの熱雑音やショット雑音はアナログ信号であり、また出力が小さいために、アナログ増幅回路の構成が大規模となり、集積化、小型化が困難である。特に、暗号セキュリティー機能を搭載したＩＣカード等の小型機器に組み込むことは困難である。
【０００６】つまり、周期性を持たない質の高い乱数を発生させ、かつ小型の集積回路が必要とされつつある。
【０００７】小型化のためには、ＴＴＬやＣＭＯＳ等の

デジタル回路で構成することが望ましい。しかし、デジタル回路は、基本的にある入力に対して同一の出力を与えるので、アルゴリズム的な処理で乱数を作ることしかできない。このため、フィードバックシフトレジスタと同様に疑似乱数しか作り出せない。

【０００８】この矛盾を解決するためには、デジタル回路で、出力が不確定になる回路を作る必要がある。

【０００９】本発明は、かかる課題の認識に基づいてなされたものである。すなわち、その目的は、真性度の高い乱数を発生させ、かつ小型の集積回路化が可能な乱数生成回路を提供することにある。

【課題を解決するための手段】上記目的を達成するため、本発明の乱数生成回路は、デジタル入力値に対して一義的に決定されないデジタル出力値を与える不確定論理回路と、前記不確定論理回路から出力される前記デジタル出力値における「０」と「１」の出現頻度を均等にするための一様化回路と、を備えたことを特徴とする。

【００１０】上記構成によれば、真性度の高い乱数を発生させ、かつ小型の集積回路化が可能な乱数生成回路を提供することができる。

【００１１】ここで、前記不確定論理回路は、フリップフロップ型の論理回路を含むものとすれば、デジタル回路で、出力が不確定になる回路として活用することができる。

【００１２】また、前記不確定論理回路は、前記フリップフロップ型の論理回路の出力を前の状態を保持した出力とするための入力信号を継続的に与えつつ、前記フリップフロップ型の論理回路の前の状態に関する情報が実質的に消去される時間あるいはそれ以上の時間に亘って前記フリップフロップ型の論理回路に対する電源をオフするフェイズと、前記フリップフロップ型の論理回路に対する電源をオンするフェィズとを交互に繰り返すことにより、前記フリップフロップ型の論理回路から不確定なデジタル信号列を出力させるものとすれば、デジタル回路で出力が不確定になる回路を実現できる。

【００１３】また、前記フリップフロップ型の論理回路は、ＲＳ型のフリップフロップであり、前記不確定論理回路は、前記ＲＳ型のフリップフロップに対する入力Ｓ及び入力Ｒとして、前の状態を保持した出力を得るための入力データの組み合わせと、フリップフロップとして無効となる入力データの組み合わせ、つまりフリップフロップの２つの出力が同じ値をとるような入力の組み合わせと、を交互に入力することにより前記ＲＳ型のフリップフロップからの出力を連続的に不確定とすれば、デジタル回路で、出力が不確定になる回路として用いることができる。

【００１４】また、前記一様化回路は、前記フリップフロップ型の論理回路から出力される「０」と「１」の出現頻度をカウントするカウント回路と、前記カウント回路によりカウントした前記出現頻度に基づいたフィードバック信号を前記フリップフロップ型の論理回路に与えるフィードバック回路と、を有するものとすれば、フリップフロップ型の論理回路からのデジタル出力列における「偏り」を抑制することができる。

【００１５】また、前記一様化回路は、前記不確定論理回路からの出力された複数のデジタル信号の排他的論理和を演算し、乱数として出力するものとすれば、「偏り」のない乱数が得られる。

【００１６】また、前記一様化回路は、「０」と「１」との出現頻度が１：１であるデジタル信号列と、前記不確定論理回路から出力されるデジタル信号列と、の排他的論理和を演算し、デジタル乱数列として出力するものとすれば、「偏り」のない乱数列が得られる。

【００１７】また、前記不確定論理回路は、４つ以上のＮＯＲ回路またはＮＡＮＤ回路を含み、これらＮＯＲ回路またはＮＡＮＤ回路は、それぞれの回路の出力端子がその次の回路の入力端子の一方に連鎖的に接続されてなるものとすれば、ウェーハ上での素子特性の「ばらつき」などによる乱数の品質の低下を防ぎ、良質の乱数を生成する乱数生成回路を安定して量産することが容易となる。

【００１８】なおここで、「連鎖的に接続」とは、例えば、４つのＮＯＲ回路を用いる場合には、第１のＮＯＲ回路の出力が第２のＮＯＲ回路の入力の一方に接続され、第２のＮＯＲ回路の出力が第３のＮＯＲ回路の入力の一方に接続され、第３のＮＯＲ回路の出力が第４のＮＯＲ回路の入力の一方に接続され、第４のＮＯＲ回路の出力が第１のＮＯＲ回路の入力の一方に接続されたような接続関係をいう。

【００１９】また、前記不確定論理回路は、複数のＲＳ型のフリップフロップを含み、これらフリップフロップ毎に大きさが異なるパルス電圧を入力し、これらフリップフロップからの出力の排他的論理的和を出力とするものとすれば、「１」と「０」の出現確率の差を確実且つ容易に小さくすることができる。つまり、「１」と「０」の出力の偏りを減らして乱数の品質を高くすることができる。

【００２０】

【発明の実施の形態】以下、図面を参照しつつ、本発明の実施の形態について詳細に説明する。

【００２１】図１は、本発明の乱数生成回路の要部構成を表すブロック図である。

【００２２】すなわち、本発明の乱数生成回路は、不確定論理回路１０と、その出力を受ける一様化回路２０とを備える。

【００２３】不確定論理回路１０は、デジタル回路で構成した論理回路であり、その論理回路の原理的にみて、特定の入力信号の組み合わせに対して出力の「０」または「１」が不確定になるものである。論理出力が不確定の場合、論理回路１０を構成する素子のその時々の物理

的な要因によって、出力が変動する。この物理現象を利用することにより、一定の入力に対して、出力が変動するデジタル回路が得られ、「０」と「１」とのランダムなデジタル信号列が得られる。

【００２４】この方法で得られた「０」と「１」とのデジタル信号列の配列は、そのデジタル回路を構成する素子の特性に依存しているので、「０」と「１」の出現頻度に「偏り」が生ずる。

【００２５】そこで、一様化回路２０において、それらを再度デジタル処理して、偏りを無くして真性度の高いデジタル乱数を得る。または、同図にフィードバックループＦとして表したように、一様化回路２０は、不確定論理回路１０の出力データに基づいたフィードバック信号を与え、出力データにおける「偏り」を抑制するようにしてもよい。

【００２６】このようにすれば、乱数生成回路を少ない論理ゲート数で構成できるので、小規模な回路で済む。「０」と「１」の頻度を補正する回路も、比較的小規模な論理回路で構成可能である。

【００２７】そして、乱数の元になる現象は、不確定論理回路１０を構成する素子の物理現象に基づくものであるので、同一の入力に対して、不確定の出力が得られるため、乱数列に周期性が出ず、乱数を推定可能な疑似乱数とは異なる質の高い乱数を得ることができる。

【００２８】以下、具体例を参照しつつ本発明の実施の形態についてさらに詳細に説明する。

【００２９】（第１の実施例）図２は、本実施例の乱数生成回路の基本構成を例示する模式図である。

【００３０】すなわち、同図の乱数生成回路は、不確定論理回路１０にＲＳ型のフリップフロップ（ＲＳ－ＦＦ）１０Ａを設けている。

【００３１】図３は、ここで用いるＲＳ－ＦＦ１０Ａの具体的な構成を例示する模式図である。同図に表したように、ＲＳ－ＦＦ１０Ａは、２つのＮＯＲ論理回路１１、１２を組み合わせたものである。

【００３２】ここで、入力Ｓ＝Ｒ＝０の場合、出力Ｑとしては、そのフリップフロップの前の出力Ｑと同じ値を出力する。しかし、電源が切れた状態が前の状態であると、再度電源を投入した後の出力は不確定となる。実際にＳ＝Ｒ＝０を入力すると、ＮＯＲ回路１１、１２を構成する複数のＣＭＯＳがＯＮ（オン）するタイミングの微妙な違いにより、「０」か「１」の出力が決まる。特性の微妙な差は常に一定ではなく、回路周囲の温度や、物理的に回路内に発生する微小な雑音などで決まるので、出力も一定でない。

【００３３】図４は、このＲＳ－ＦＦの動作を表すパルス図である。

【００３４】ここで、Ｓ＝Ｒ＝０としたまま、パルス的にＮＯＲ回路１１、１２の電源電圧Ｖｃｃ（Ｖｉｎ）をＯＮ、ＯＦＦすることを、それぞれ「０」、「１」の入力とする。フリップフロップの情報を完全に消去するのに十分な時間だけ「０」を入力した後、「１」を入力することによりフリップフロップの出力を不確定にすると、「１」の入力に対して、不確定な出力Ｑが得られる。従って、このように入力として「０」と「１」とを繰り返すと、図４に表したように出力Ｑとして、「０」または「１」の不確定でランダムな数値列が得られる。

【００３５】但し、論理回路１１、１２を構成するトランジスタが完全には対称ではないため、「０」と「１」の出現頻度は均等でなく、どちらかに偏る。そこで、後述するように、「０」と「１」を均等にする回路２０と組み合わせることにより、本発明の乱数生成回路が得られる。

【００３６】なお、インバータを配列したデジタル回路を用いて乱数的なデジタル信号を生成させるものとしては、例えば、特開２００１－１６６９２０号公報に開示されているように、デジタル回路に付加する素子の温度変動を用いるものがある。しかし、この従来技術の場合には、奇数個のインバータを環状接続したリングオッシレータの発振周波数を温度に対して不安定にさせる点で、本願とは全く異なる。さらに、この従来技術の場合、全体構成が複雑で回路規模が大きいという点でも改善すべき点は多い。また、リングオッシレータなどの正帰還型発振回路の場合、発振を開始するトリガーが、回路の基本クロックと同期したノイズ信号であるので、発振回路とクロックを完全に非同期にできないため、発生する乱数列に周期性が現れて、乱数の真性度が損なわれるという問題がある。

【００３７】これに対して、本発明によれば、フリップフロップの不確定出力を積極的に作り出すことにより、はるかにコンパクトで効率的に乱数デジタル信号列を得ることができる。

【００３８】さて、本発明においてＲＳ型のフリップフロップを用いる場合、図５のように２つのＮＯＲ論理回路１１、１２を接続すると、上記具体例とは違った方式で不確定の出力を得ることができる。

【００３９】図６は、その動作を説明するパルス図である。

【００４０】この場合、電源Ｖｃｃは通常どおりＯＮにしておき、入力をＳ＝Ｒとして、図６に表したように、「１」と「０」を交互に入力する。Ｓ＝Ｒ＝０の場合は、出力Ｑは前の状態のＱを保持し、出力／Ｑ（「Ｑバー」を表す）は前の状態のＱを保持して、それぞれ「０」か「１」の値をとる。

【００４１】ところが、Ｓ＝Ｒ＝１の場合、Ｑ＝０と／Ｑ＝０で同じになってしまうので、その次にＳ＝Ｒ＝０とするとＱは１となるか、０となるか不確定となる。その結果として、図６に表したような不確定なデジタル信号列が得られる。

【００４２】但し、この場合にも、得られるデジタル信

号列において、「０」と「１」との出現頻度は均等ではない場合が多いので、後述する「０」と「１」を均等にする回路２０と組み合わせられることにより、本発明の乱数生成回路が得られる。

【００４３】また、本発明の乱数生成回路における不確定論理回路１０としては、図２乃至図６に表した具体例以外にも、これと同様に、Ｄ型フリップフロップの場合にはクロック入力を「０」に、ＪＫフリップフロップの場合にはＪ＝Ｋ＝１または０に、またＴ型の場合には入力Ｔを任意の値にしておけば、フリップフロップの初期値が決まっていない場合に出力が不確定となり、上記と同様にして乱数生成回路を構成することができる。他の種類のフリップフロップも同様であり、要は、不確定な出力が利用できればよい。

【００４４】（第２の実施例）次に、本発明の第２の実施例について説明する。

【００４５】図７は、本実施例の乱数生成回路の不確定論理回路１０の要部を表す模式図である。

【００４６】すなわち、本実施例においては、不確定論理回路において、２つのＣＭＯＳ回路１３、１４を並べ、ゲートとＣＭＯＳのトランジスタの間を相互に結線したフリップフロップ回路１０Ｃを設ける。これは、ＭＯＳトランジスタＴ１がＯＮすると、ＭＯＳトランジスタＴ３がＯＦＦするフリップフロップである。

【００４７】図８は、このフリップフロップ回路の動作を説明する模式図である。

【００４８】電源を切っている状態では、全てのトランジスタはＯＦＦであり、どの電極の電位もグランドと同じである。

【００４９】そして、Ｖｉｎを１（Ｈ：High）とすると、各トランジスタのゲートの電位は０（Ｌ：Low）であるので、トランジスタＴ１とトランジスタＴ３がＯＮ状態になりうるが、フリップフロップであるので、どちら一方のみがＯＮ状態となる。

【００５０】仮に図８（ａ）に表したように、トランジスタＴ１が先にＯＮしたとすると、トランジスタＴ１のソースとドレインは導通して等電位となり、Ａ点の電位はＶｉｎと同じＨｉｇｈレベルになる。そうすると、トランジスタＴ３はＯＦＦとなり、トランジスタＴ４がＯＮ状態となって安定化する。このときＢ点の電位、すなわち出力は初期のＬｏｗ（０）のままである。

【００５１】逆に、トランジスタＴ３が先にＯＮしたとすると、図８（ｂ）に表した状態となり、出力はＨｉｇｈ（１）となる。

【００５２】このように、トランジスタＴ１とＴ３のどちらが早くＯＮするかで、出力が決まる。どちらが速くＯＮするかは不確定であり、前述した第１実施例と同様に出力が不確定なフリップフロップとなる。フリップフロップの電源のＯＮ、ＯＦＦを「０」、「１」のデジタル入力とすると、入力「１」に対して、「０」か「１」が不確定の出力を出す。

【００５３】ただし、２つのＣＭＯＳが完全に同一の特性を持っていないので、Ｔ１とＴ３のどちらが早くＯＮするかには偏りが出る。これを、以下に詳述するように、一様化回路２０により補正すれば、真性度の高いデジタル乱数を得ることができる。

【００５４】（第３の実施例）次に、本発明の第３の実施例として、一様化回路２０の具体例について詳細に説明する。

【００５５】前述した第１及び第２実施例においては、不確定論理回路１０の具体例としてフリップフロップ回路を用いた。しかし、前述したように、これらフリップフロップ回路から得られるデジタル信号列は、「０」と「１」の出現頻度が完全に均等ではなく、ある種の「偏り」を持っている。一様化回路２０は、この「偏り」を補正するためのデジタル処理を行う。

【００５６】図９は、本実施例における一様化回路の動作を説明するための概念図である。

【００５７】同図に表したように、不確定論理回路１０の出力を時系列的に、Ｑｎ、…Ｑｎ＋ｋとして、これらのｋ＋１個のデータにＸＯＲ（排他的論理和）の論理演算を施す。その結果をＴとする。不確定論理回路１の出力において、「１」の出現確率をｐ、「０」の出現確率を１－ｐとすると、Ｔが１となる確率は、

０．５＋０．５・（１－２ｐ）$^{k+1}$

となる。ｋが大きくなるほど、確率が０．５に近づき、偏りが補正される。

【００５８】前述した第１実施例において実際に試作したＲＳ－ＦＦでは、「偏り」が大きくほぼｐ＝０．１であった。ｋ＝１０の場合、Ｔが１となる確率は０．５４３となり、またＫ＝２０の場合、０．５０５となり、またＫ＝３０の場合、０．５００５となって、０．５に近づき、ほとんど「偏り」がなくなる。

【００５９】ｋが大きくなると、乱数の生成速度が遅くなってしまうが、例えば電源をＯＮ、ＯＦＦする周期を３０ＭＨｚにすると、ｋ＝３０としても約１Ｍｂｉｔ／秒の速度でデジタル乱数列を生成することができるので、実用上は問題とならない場合が多い。または、Ｑｎ、…Ｑｎ＋ｋのＸＯＲ、Ｑｎ+1、…Ｑｎ＋ｋ+1のＸＯＲＱｎ+2、…Ｑｎ＋ｋ+2のＸＯＲというように、一つづつ、ずらして演算すれば、生成速度も損なわない。

【００６０】また、このようにして得られた乱数列データをフィードバックシフトレジスタのシード（種）に使っても良い。

【００６１】また、以下に説明するような方法を用いれば、簡便に「０」と「１」の出現確率を均等にすることができる。

【００６２】すなわち、デジタル信号Ｐが「１」になる確率をｐ、デジタル信号Ｑが「１」になる確率をｑとすると、ＰとＱとの排他的論理和（ＸＯＲ）の演算値Ｔが

「１」となる確率と、「０」となる確率の差は、次式により表される。
４（０．５－ｐ）（０．５－ｑ）・・・（１）
従って、「Ｐが「１」になる確率が０．５」であれば、Ｑが「１」になる確率が０．５でなくても、ＰとＱとの排他的論理和の演算値Ｔの「０」と「１」の出現確率は等しくなる。
【００６３】ここで、図１０に表したように、フリップフロップ１０への入力信号を分岐してＴ型のフリップフロップ２０Ｂに入れると、周期が２倍の信号になり、これはフリップフロップ１０の出力と同じタイミングで「０」と「１」とが交互に並ぶ信号となる。この信号は、当然に「０」と「１」の出現率が等しい。従って、この信号とフリップフロップ１０の信号との排他的論理和をとると、その演算出力Ｔにおいては当然に「０」と「１」の出現確率が等しく、真性度の高いデジタル乱数列として用いることができる。
【００６４】また、図１１に表したように、フィードバックシフトレジスタ（ＦＳＲ）２０Ｃにより、フリップフロップ１０と同じクロックで作った擬似乱数Ｒは、「０」と「１」とを均等に出力するので、これとフリップフロップ１０の出力との排他的論理和をとると、その演算値Ｔは「０」と「１」の出現率が等しく、真性度の高いデジタル乱数列として用いることができる。
【００６５】また、２つのフリップフロップを利用した構成として、もうひとつの具体例を挙げることができる。
【００６６】図１２は、この具体例を表す模式図である。すなわち、Ｔ型フリップフロップで倍周期にしたものと、Ｄ型フリップフロップで均一化したものをＸＯＲする。
【００６７】この場合には、２個の不確定フリップフロップ回路Ａ及びＢを使う。まず、基準クロック信号を２分割して、一方をＴ型フリップフロップに通して、周期が１／２になるようにして不確定フリップフロップＡに入力する。すると、基準クロックの１／２周期の不確定ランダム信号Ａが得られるが、「０」と「１」の出現率は、この段階では不均一である。
【００６８】もう一方は、不確定フリップフロップＢに通して、不確定出力ＱとＱバーを得る。Ｑバーをｄ型フリップフロップに通して、基準クロック一つ分遅らせてから、ＱとＱバーを交互に出力すると、この信号は原理的に「０」と「１」とが５０パーセントづつ配列するランダム信号Ｂとなる。但し、ＱとＱバーが順番に並ぶので、この時点では規則性が現れる。こうして作ったランダム信号ＡとランダムＢとの排他的論理和（ＸＯＲ）をとると、先の２例と同様の原理で、０と１の出現率が均一な乱数が得られる。
【００６９】（第４の実施例）次に、本発明の第４の実施例として不確定論理回路の出力をモニタしフィードバックをかける乱数生成回路について説明する。
【００７０】図１３は、本実施例の乱数生成回路の要部構成を表す模式図である。
【００７１】本実施例においては、第１及び第２の実施例として前述したような不確定フリップフロップの入力部に、一様化回路２０がフィードバックを加える。このようなフィードバックにより、不確定フリップフロップの「０」と「１」の出現確率を均等に近くすることができる。
【００７２】すなわち、同図において、Ａ側にあるトランジスタＴ７が早くＯＮすると、フリップフロップの出力が「０」になるとする。同図に表したように、フィードバック回路２０Ｅと電源入力Ｖｉｎとの間に同一の設計仕様を持つＮチャネルのＭＯＳトランジスタＴ７、Ｔ８をそれぞれ設け、Ｂ側のトランジスタＴ８のゲートはグランドに落としておく。
【００７３】フリップフロップの出力をデジタルカウンタ２０Ｄでカウントしておき、「０」と「１」のカウントの差分に比例した電圧をＡ側のＭＯＳトランジスタＴ７のゲートに与え、「１」の出力が多い場合に、Ａ側のトランジスタＴ７のゲート電圧を少しプラスにシフトしてチャネル抵抗を相対的に低くして、Ａ側に電流が流れやすくすると、Ａ側が優先的に動作するので、出力「０」が増える。
【００７４】逆に、「０」の出力が多い場合には、Ａ側のトランジスタＴ７のゲート電圧をマイナスにして、チャネル抵抗を上げる。
【００７５】こうしたフィードバックをかけることにより、フリップフロップの出力の「０」と「１」のずれを少なくすることができる。その結果、このまま乱数として使うことも出きる。
【００７６】また、第３実施例として説明したように、「偏り」をなくす論理回路を組み合わせると、乱数の「偏り」をさらに小さくできる。この場合、前述したＸＯＲをとるデータｋの数が少なくて済むので、乱数の生成速度を上げることができる。
【００７７】（第５の実施例）次に、本発明の第５の実施例として、不確定論理回路１０において、フリップフロップを構成するＮＯＲ回路（またはＮＡＮＤ回路）の数を増やすことで、「０」と「１」の出力の偏りを減らす構成について説明する。
【００７８】半導体回路を量産する場合、ウェーハ上での特性の「バラツキ」などにより、一部の出力に極端に偏りなどが生ずる場合がある。例えば、「０」の出現頻度が１００パーセントにほぼ近くなるという回路が、全体の一部に出現する可能性がある。出力が極端に偏ると、平滑回路で補正しても乱数の質が高まらないため、乱数生成回路としては不良品となる。本実施例は、この不良品の出現を減らすために用いて好適なものである。
【００７９】図１４は、本実施例の構成を概念的に表す

模式図である。本実施例においては、偶数個のフリップフロップからの出力のＸＯＲをとる。すなわち、多数（偶数）のＮＯＲ回路（またはＮＡＮＤ回路）を図１４の例示したように並べ、それぞれのＮＯＲ回路の出力がその次のＮＯＲ回路の入力の一方となるように連鎖的に接続した場合、不確定フリップフロップと同様の動作を行わせることができる。

【００８０】つまり、入力（Input）が「１」の場合、各フリップフロップの出力は全て「０」となる状態が安定である。つまり、入力「１」は、リセット（Ｒ）信号であるといえる。続いて、入力を「０」にすると、ＮＯＲ回路は、インバータと等価となるので、「１」と「０」が交互に出力される状態が安定である。つまり、入力「０」は、セット（Ｓ）信号であるといえる。そして、これらＮＯＲ回路からの出力が、順に「０」、「１」、「０」、「１」となるか、それとも、「１」、「０」、「１」、「０」となるかは、その前の状態を保持することにより決定されるが、その前の状態（入力として「１」を与えた状態）における出力が、「０」、「０」、「０」、「０」であるため、どちらになるか不確定となる。

【００８１】この場合、多数のＮＯＲ回路が競合状態となるので、２つのＮＯＲ回路でフリップフロップを構成する場合よりも、出力の偏りが小さくなる。当然ながら、ＮＯＲ回路の数が多いほど、出力の偏りも小さくなる。

【００８２】この具体例の場合、奇数番目のＮＯＲ回路の出力どうしと、偶数番目のＮＯＲ回路の出力どうしは、原理的に同じ出力値となる。偶数番目または奇数番目の出力を前述した一様化回路と組み合わせることで、さらに良質の乱数を得ることができる。

【００８３】次に、本実施例の第２の具体例として、偶数個のフリップフロップに発振回路からの信号を入力する構成について説明する。

【００８４】図１５は、本具体例の要部構成を例示する模式図である。すなわち、同図（ａ）に表したように、多数かつ偶数個のＮＯＲ回路（またはＮＡＮＤ回路）を並べて不確定フリップフロップを形成し、それぞれのＮＯＲ回路への入力を同図のように独立化させる。そして、それぞれに、「０」か「１」のいずれかと、「０」と、を交互に入力する。このようにすると、さらにランダム化の要素が増えるため、良質な乱数を作ることができる。

【００８５】以下、この原理を図１５のように４つのＮＯＲ回路からなる場合について説明する。各ＮＯＲ回路への入力と出力の組合せを、便宜的に（Ｘ１、Ｘ２、Ｘ３、Ｘ４：Ｑ１、Ｑ２、Ｑ３、Ｑ４）と表すとすると、例えば、以下の如くとなる。

（１、０、０、０：０、１、０、１）
（１、１、０、０：０、０、１、０）
（１、０、１、０：０、１、０、１）
（１、０、０、１：０、１、０、０）
（１、１、１、０：０、０、０、１）

この時の出力Ｑ１～Ｑ４が、「０」と「１」とが交互に並ばない場合には、この次に、入力Ｘとして全て「０」を入力すると、ＮＯＲ型回路は全てインバータと等価になるため、Ｘ及びＱは、以下のいずれかとなる。

（０、０、０、０：０、１、０、１）
または（０、０、０、０：１、０、１、０）

この場合、そのどちらになるかは、不確定である。入力Ｘがランダム性を持っていると、不確定フリップフロップのランダム性との相乗効果により、乱数の質が向上する。ランダム入力のひとつの方法として、図１６に例示したように、非同期で周波数の異なる発振回路を用いる方法が有効である。

【００８６】すなわち、ＮＯＲ回路のそれぞれに対応させて、非同期発振回路とＤ型ラッチを設ける。ここで、非同期発振回路は、その出力が「０」か「１」に変換されるように、出力端にバッファがついたものが望ましいが、マルチバイブレータのように出力がデジタル化されている場合には不用である。非同期発振回路からの出力は、標準クロックに合わせてラッチされ、そのラッチ信号とクロックのＡＮＤをとると、「０」か「１」のいずれかと、「０」と、が交互に並んだ信号が得られる。これらを入力Ｘとすれば、フリップフロップからの出力は、図１５（ｂ）に例示したように、確定値である「０」と、不確定値としての「０」か「１」のいずれか、を交互に出力する。不確定値を取り出すことで、デジタル乱数が得られる。

【００８７】なおここで、Ｘ１からＸ４の独立入力を適当な確定出力を与える論理回路で処理しただけでは乱数は作ることはできない。非同期であっても、各入力Ｘに周期性があるため、それらを論理回路で組み合わせただけでは、出力に必ず周期性が表れ、良質の乱数は一般に得られない。不確定フリップフロップを介して、始めて良質の乱数となる。

【００８８】または、図１７に例示したように、擬似乱数を発生するＬＦＳＲ（Linear Feedback Shift Resistor）を使い、いずれかのシフトレジスタＳＲからランダム入力する方法も簡便で有効である。図１７では、図１６と違いNAND回路が２段で接続されているが、これは論理動作として、AND回路とNOR回路が２段で接続されている場合と、同様のものである。

【００８９】原理的に、出力の奇数番目どうしと、偶数番目どうしは、同じ出力値となる。偶数番目または奇数番目の出力を前述した一様化回路２０と組み合わせることで、さらに良質の乱数を得ることができる。

【００９０】（第６の実施例）次に、本発明の第６の実施例として、前述した第５実施例とは別の方法により、不確定論理回路１０において、フリップフロップを構成

するＮＯＲ回路（またはＮＡＮＤ回路）の数を増やして、「０」と「１」の出力の偏りを減らす構成について説明する。

【００９１】図１８は、本実施例の回路の要部を表す模式図である。同図（ａ）は、５つのＵＦＦにより構成した具体例を表す。ここで、ＵＦＦ（Unsettlable Flip-Flop）は、同図（ｂ）に例示したように、ＮＯＲ回路２個からなる不確定フリップフロップとすることができる。

【００９２】ＵＦＦは、「０」と「１」の出力頻度が、入力パルス電圧の高さに依存する傾向がある。すなわち、入力パルスをデジタル回路の基準となる電源電圧ＶDDよりも小さくしていくと、ＵＦＦには、「１」の出力頻度が高くなっていくか、あるいは、低くなっていく傾向が見られる。これは、ＵＦＦを構成するそれぞれのＮＯＲ回路の閾値電圧に、小さいながらも「ばらつき」が存在するためである。

【００９３】図１９は、ＵＦＦに入力するパルス電圧に対する「１」の出現確率の依存性を例示するグラフ図である。すなわち、同図の具体例の場合、入力パルスの周期を２マイクロ秒、パルス幅を６５ナノ秒とし、そのパルス電圧Ｖｒｓを変化させた時の、ＵＦＦ出力の「１」の出現確率を表す。またこのＵＦＦは、電源電圧ＶDDが２ボルトのものである。

【００９４】図１９から、パルス電圧Ｖｒｓが高くなるに従って、「１」の出現確率が連続的に増加していることが分かる。そして、パルス電圧Ｖｒｓがおよそ１．３ボルト弱の時に、「１」の出現確率がほぼ０．５となる。つまり、このパルス電圧を与えた場合、ＵＦＦの出力における「０」と「１」の出現確率はほぼ同一となる。

【００９５】従って、図１８に例示したように、複数個のＵＦＦのそれぞれに異なった電圧のパルスを入力すると、いずれかのＵＦＦにおいて、「０」と「１」の出力頻度の差が比較的小さい出力が得られる。

【００９６】図１８においては、５つのＵＦＦに対する入力電圧を、ＶDDから、ＶDDの２０パーセントまで順に減らしている。５つのＵＦＦの出力の排他的論理和ＸＯＲをとると、このＸＯＲの出力の「０」と「１」の出力頻度の差は、５つのＵＦＦの中で「０」と「１」の出力頻度の差が一番小さいものと同程度か、それよりも小さくなる。この原理は、図９に例示した一様化回路２０ＡのＸＯＲの作用として前述したものと同様である。図１８は、５つのＵＦＦを用いた場合を例示するが、ＵＦＦの数を増やして、それらの電源電圧を細かく変化させるほど、「０」と「１」の出力の偏りを減らす効果が高まる。

【００９７】以上、具体例を例示しつつ本発明の実施の形態について説明した。しかし、本発明は、上述した各具体例に限定されるものではない。

【００９８】例えば、本発明において用いる不確定論理回路および一様化回路の具体的な構成に関しては、上記の具体例に限定されず、その機能あるいは作用が同様な全ての回路に置換したものも本発明の範囲に包含される。

【００９９】例えば、出力が不確定なフリップフロップを複数個、並列もしくは直列に並べた論理回路の出力を、「０」と「１」とを均等にする論理回路に入力する形式の乱数生成回路も、同様に有効であり、本発明の範囲に包含される。

【０１００】さらに、前述した複数の実施例のうち、不確定出力のデジタル回路と、デジタル出力の頻度を補正する回路とを部分的に組み合わせたものも、乱数生成回路として使用可能であり、本発明の範囲に包含される。

【０１０１】また、本発明の乱数生成回路によって作られたデジタル乱数は、そのまま使用することもできるが、フィードバックシフトレジスタの種として用いることにより、新たな乱数を生成することもできる。

【０１０２】

【発明の効果】以上詳述したように、本発明によれば、フリップフロップ型の論理回路などを利用することにより、乱数生成回路を少ない論理ゲート数で構成できるので、小規模な回路で済む。

【０１０３】また同時に、「０」と「１」の頻度を補正する一様化回路も、比較的小規模な論理回路で構成可能である。

【０１０４】そして、乱数の元になる現象は、不確定論理回路を構成する素子の物理現象に基づくものであるので、同一の入力に対して、不確定の出力が得られるため、乱数列に周期性が出ず、乱数を推定可能な疑似乱数とは異なる質の高い乱数を得ることができる。

【０１０５】さらに、一定周期のクロック信号を分岐してＴ型のフリップフロップなどにより不確定論理回路の出力と同じタイミングで「０」と「１」とが交互に並ぶ信号を形成し、この信号と不確定論理回路の出力信号との排他的論理和をとると、その演算出力Ｔにおいては当然に「０」と「１」の出現確率が等しく、真性度の高いデジタル乱数列として用いることができる。

【０１０６】すなわち、本発明によれば、真性度が高い乱数をコンパクト且つ低価格で実現できるようになり、例えばＩＣカードなどに応用してセキュリティーの確実な安価なカードシステムを実現できる点で産業上のメリットは多大である。

【図面の簡単な説明】

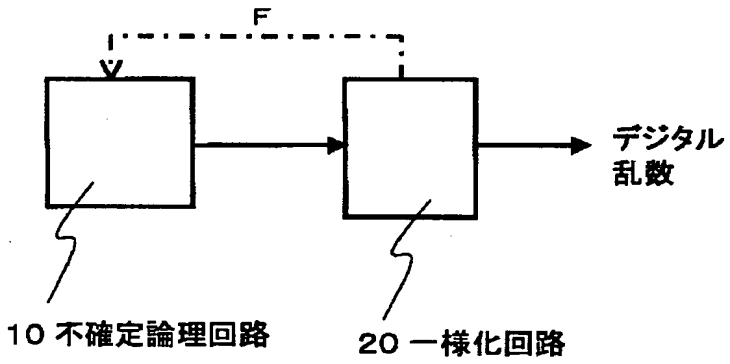
【図１】本発明の乱数生成回路の要部構成を表すブロック図である。

【図２】本発明の実施例の乱数生成回路の基本構成を例示する模式図である。

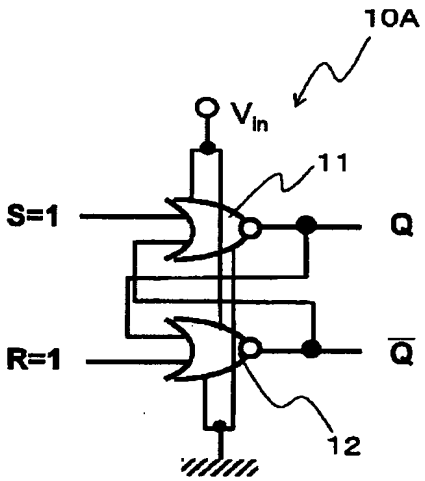
【図３】本発明の第１実施例において用いるＲＳ－ＦＦ１０Ａの具体的な構成を例示する模式図である。

【図４】ＲＳ－ＦＦの動作を表すパルス図である。
【図５】２つのＮＯＲ論理回路１１、１２を接続したＲＳ－ＦＦのもうひとつの具体例を表す模式図である。
【図６】図５のＲＳ－ＦＦの動作を説明するパルス図である。
【図７】本発明の実施例の乱数生成回路の不確定論理回路１０の要部を表す模式図である。
【図８】本発明の実施例のフリップフロップ回路の動作を説明する模式図である。
【図９】本発明の実施例における一様化回路の動作を説明するための概念図である。
【図１０】一様化回路のもうひとつの具体例を表す模式図である。
【図１１】一様化回路のもうひとつの具体例を表す模式図である。
【図１２】２つのフリップフロップを利用したもうひとつの具体例を表す模式図である。
【図１３】本発明の実施例の乱数生成回路の要部構成を表す模式図である。
【図１４】本発明の第５実施例の構成を概念的に表す模式図である。
【図１５】本発明の第５実施例の具体例の要部構成を例示する模式図である。
【図１６】ランダム入力のひとつの方法として、非同期で周波数の異なる発振回路を用いた構成を表す模式図である。
【図１７】擬似乱数を発生するＬＦＳＲ（Linear Feedback Shift Resistor）を使い、いずれかのシフトレジスタＳＲからランダム入力する構成を表す模式図である。
【図１８】本発明の第６実施例の回路の要部を表す模式図である。
【図１９】ＵＦＦに入力するパルス電圧に対する「１」の出現確率の依存性を例示するグラフ図である。
【符号の説明】
１０ 不確定論理回路
１０Ａ～１０Ｃ フリップフロップ型の論理回路
１１、１２ ＮＯＲ型論理回路
１３、１４ ＭＯＳトランジスタ
２０ 一様化回路
２０Ａ ＸＯＲ回路
２０Ｂ Ｔ型フリップフロップ
２０Ｃ ＦＳＲ
２０Ｄ デジタルカウンタ
２０Ｅ フィードバック回路

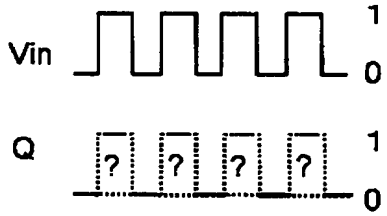
【図１】



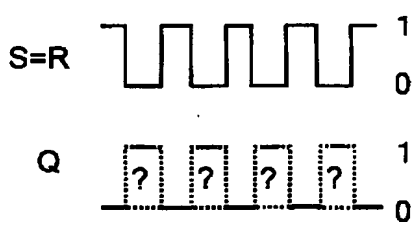
【図３】



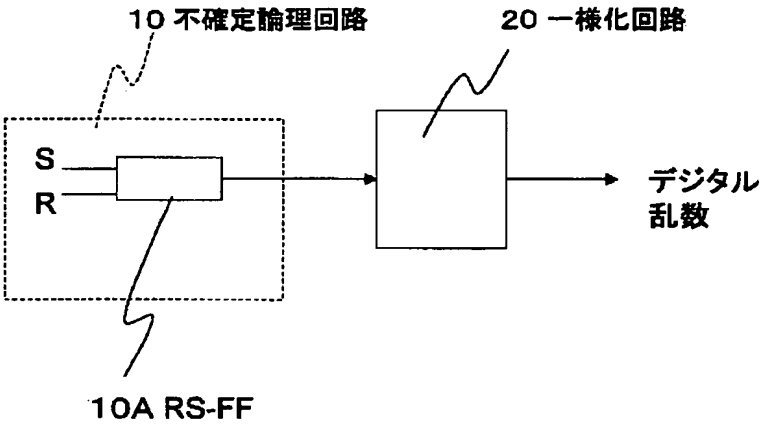
【図４】



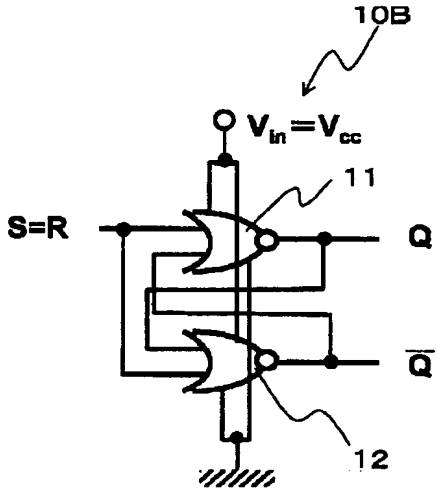
【図６】



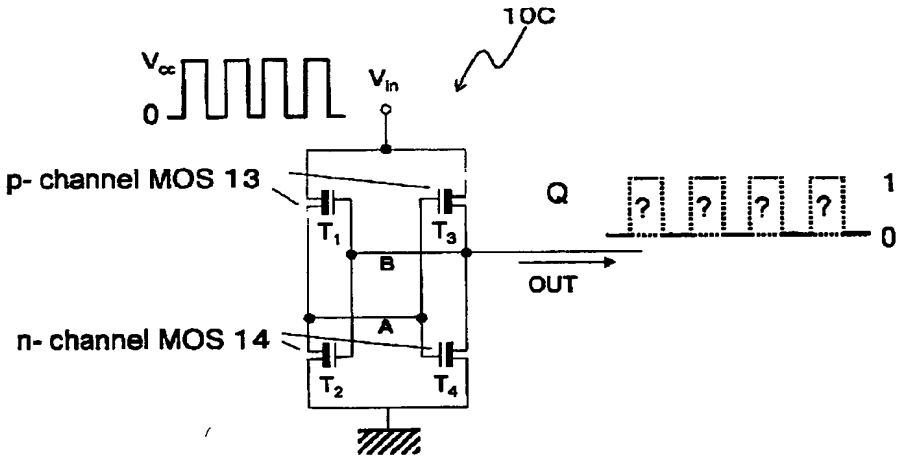
【図２】


10 不確定論理回路
20 一様化回路
S
R
デジタル
乱数
10A RS-FF

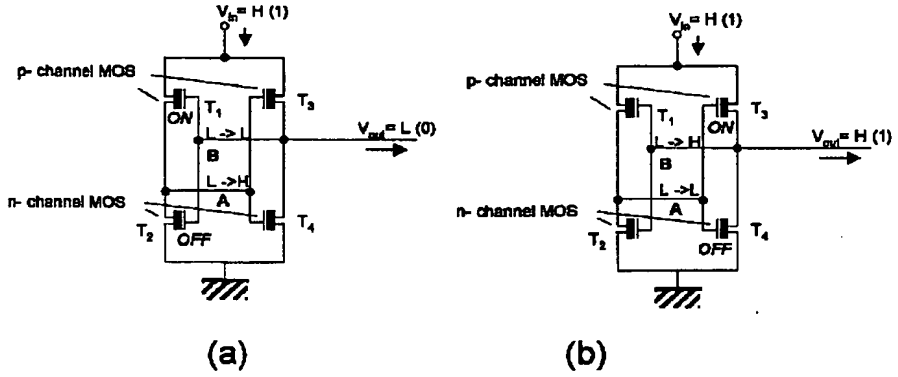
【図５】


10B
$V_{in}=V_{cc}$
11
S=R
Q
$\overline{Q}$
12

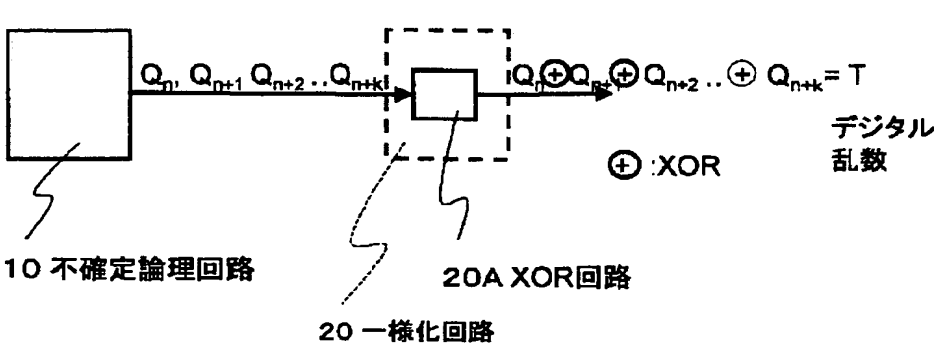
【図７】


10C
V_{cc}
0
V_{in}
p- channel MOS 13
n- channel MOS 14
T_1
T_2
T_3
T_4
A
B
Q
OUT
1
0

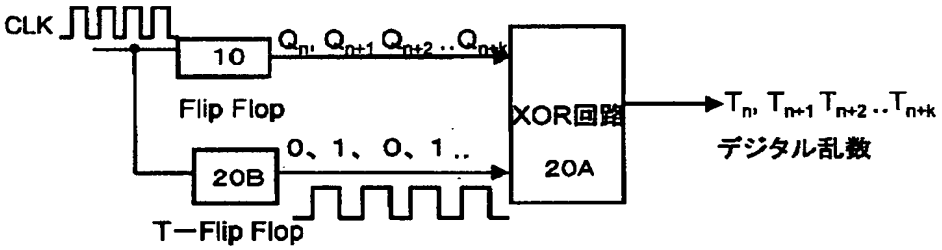
【図８】


V_{in}= H (1)
p- channel MOS
n- channel MOS
ON
OFF
L ->H
L ->L
V_{out}= L (0)
V_{out}= H (1)
(a)
(b)

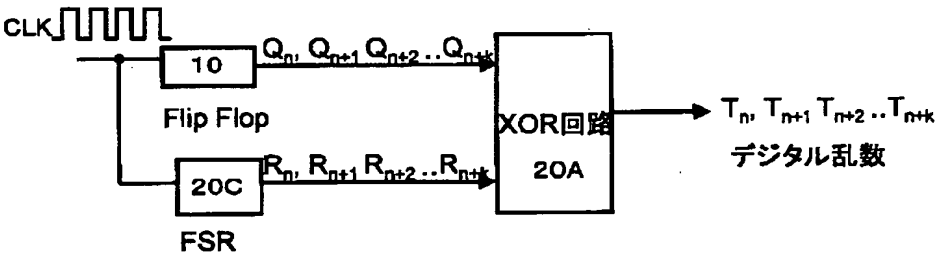
【図９】



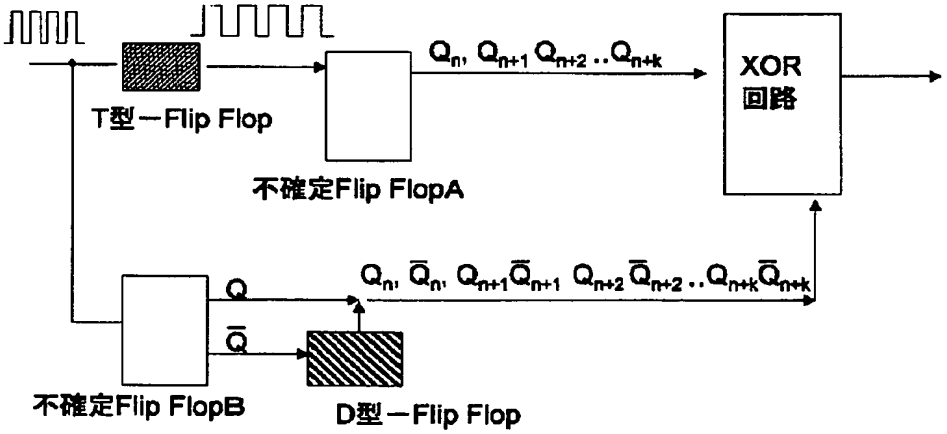
【図１０】



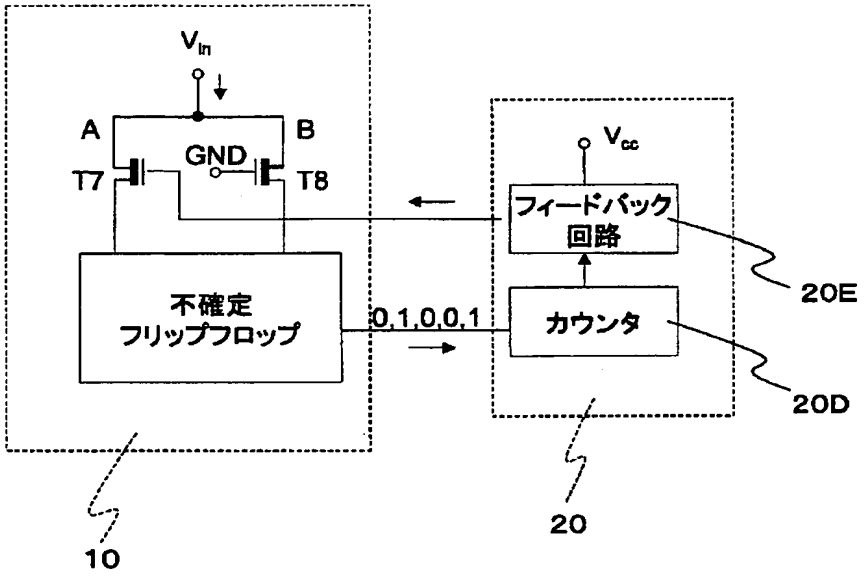
【図１１】



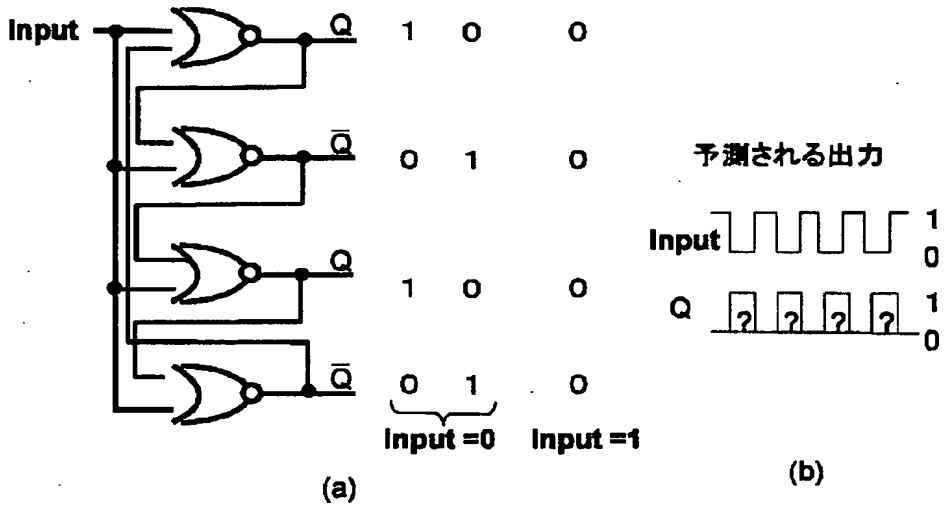
【図１２】



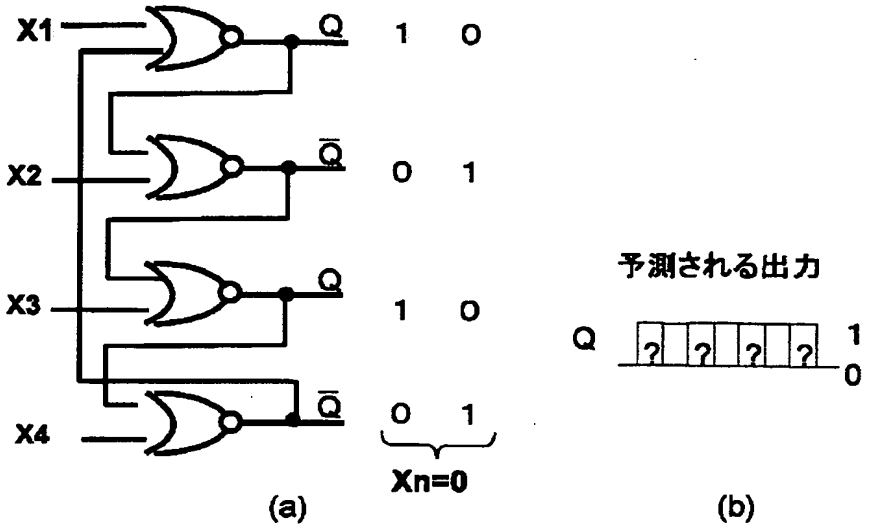
【図１３】


V_{in}
A
B
GND
T7
T8
不確定
フリップフロップ
0,1,0,0,1
V_{cc}
フィードバック
回路
カウンタ
20E
20D
10
20

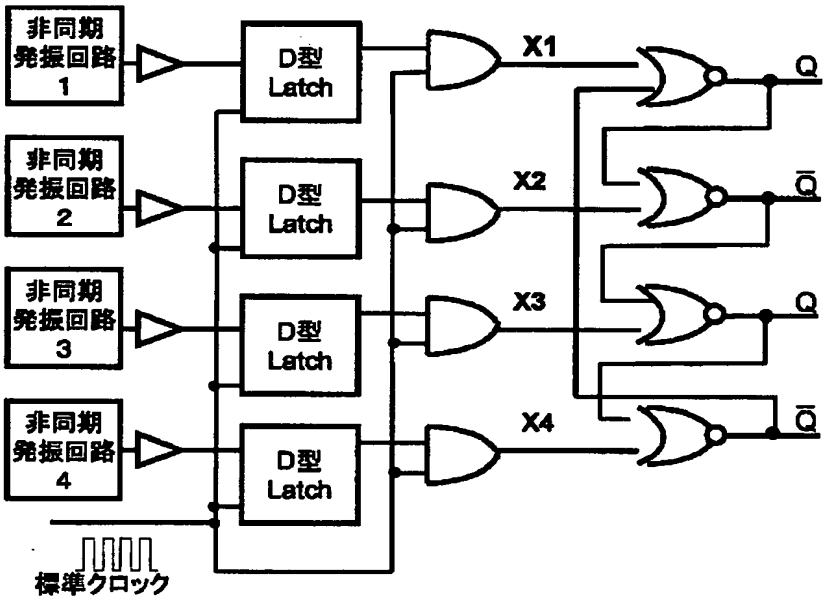
【図１４】


Input
Q
$\overline{Q}$
Q
$\overline{Q}$
1 0 0
0 1 0
1 0 0
0 1 0
Input =0
Input =1
(a)
予測される出力
Input
Q
1
0
?
(b)

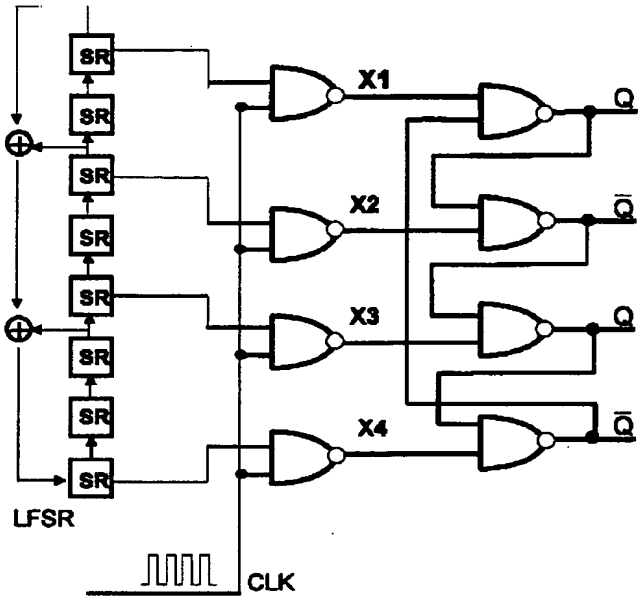
【図１５】


X1
X2
X3
X4
Q
1 0
0 1
1 0
0 1
Xn=0
(a)
予測される出力
Q
? ? ? ?
1
0
(b)

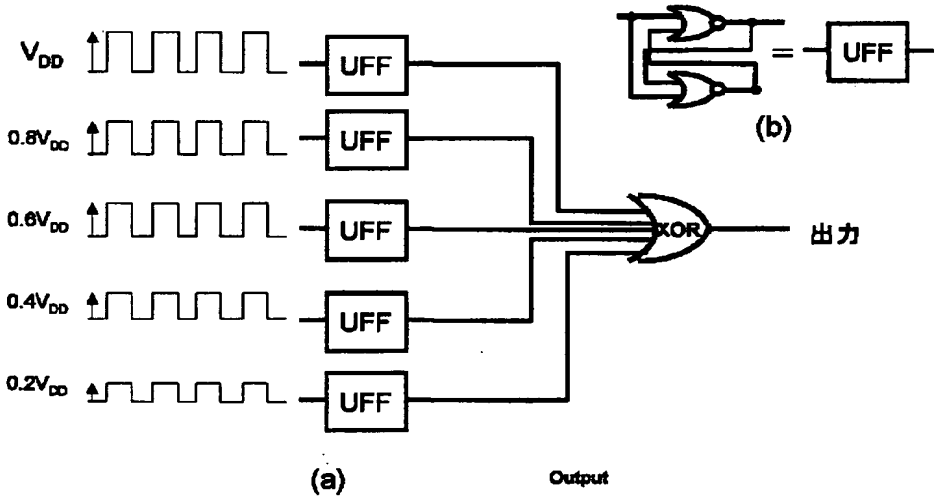
【図１６】


非同期発振回路1
非同期発振回路2
非同期発振回路3
非同期発振回路4
D型Latch
D型Latch
D型Latch
D型Latch
X1
X2
X3
X4
Q
標準クロック

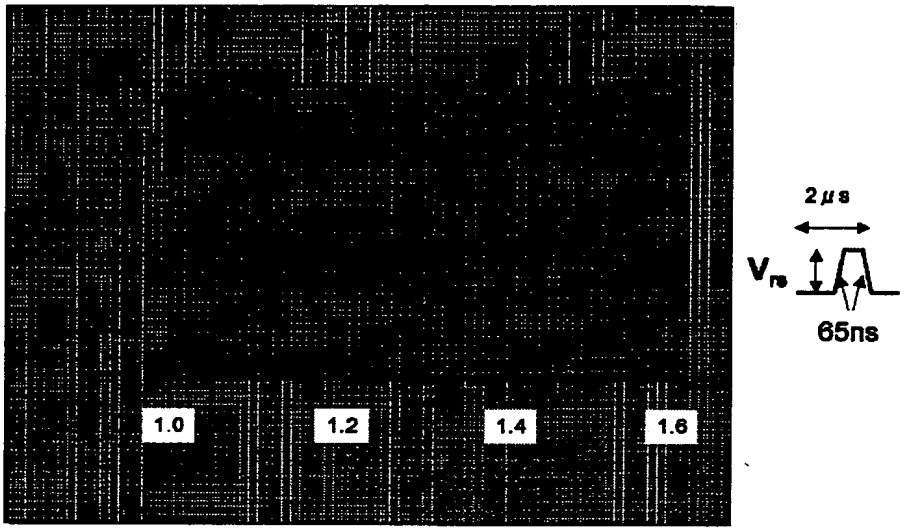
【図１７】


SR
SR
SR
SR
SR
SR
SR
SR
LFSR
X1
X2
X3
X4
Q
$\bar{Q}$
Q
$\bar{Q}$
CLK

【図１８】


V_{DD}
$0.8V_{DD}$
$0.6V_{DD}$
$0.4V_{DD}$
$0.2V_{DD}$
UFF
UFF
UFF
UFF
UFF
XOR
出力
(a)
Output
=
UFF
(b)

【図１９】



フロントページの続き

(72)発明者　古賀　淳二
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝横浜事業所内

(72)発明者　大場　竜二
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝横浜事業所内

Ｆターム(参考)　5J049 CA03 CA10
5J104 FA01 NA04

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成16年10月7日(2004.10.7)

【公開番号】特開2003-173254(P2003-173254A)
【公開日】平成15年6月20日(2003.6.20)
【出願番号】特願2002-183967(P2002-183967)
【国際特許分類第７版】
　Ｇ０６Ｆ　7/58
　Ｇ０９Ｃ　1/00
　Ｈ０３Ｋ　3/84
【ＦＩ】
　Ｇ０６Ｆ　7/58　A
　Ｇ０９Ｃ　1/00　６５０Ｂ
　Ｈ０３Ｋ　3/84　Z

【手続補正書】
【提出日】平成15年9月25日(2003.9.25)
【手続補正１】
【補正対象書類名】図面
【補正対象項目名】図３
【補正方法】変更
【補正の内容】

【図３】